PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/08 — A1

(11) International Publication Number: WO 00/01109

(43) International Publication Date: 6 January 2000 (06.01.00)

(21) International Application Number: PCT/CA99/00595

(22) International Filing Date: 28 June 1999 (28.06.99)

(30) Priority Data:
2,241,705 26 June 1998 (26.06.98) CA

(71) Applicant *(for all designated States except US)*: CERTICOM CORP. [CA/CA]; Suite 103, 200 Matheson Boulevard West, Mississauga, Ontario L5R 3L7 (CA).

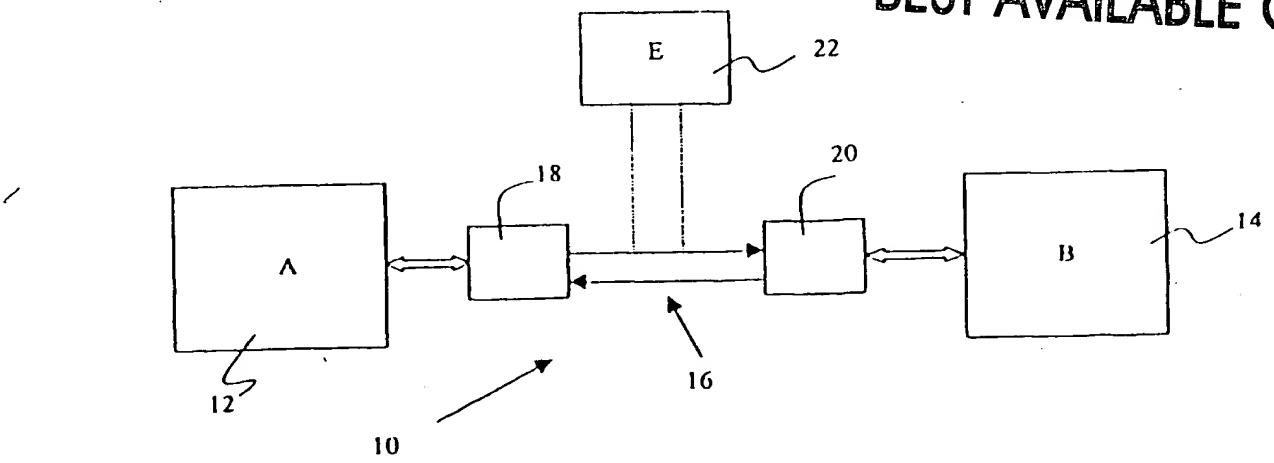
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: MENEZES, Alfred, J. [CA/CA]; Apartment 1604, 6 Willow Street, Waterloo, Ontario N2J 4S3 (CA). BLAKE-WILSON, Simon [CA/CA]; 237 Montrose Avenue, Toronto, Ontario M6G 3G6 (CA).

(74) Agents: PILLAY, Kevin et al.; Orange Chari Pillay, Toronto Dominion Bank Tower, Suite 3600, Toronto-Dominion Centre, P.O. Box 190, Toronto, Ontario M5K 1H6 (CA).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A METHOD FOR PREVENTING KEY SHARE ATTACKS



(57) Abstract

A key agreement protocol for preventing key-share attacks wherein a method is provided for establishing a common shared key between a pair of correspondents in a station-to-station protocol by exchanging messages between the correspondents and including identification information in said messages, said information being identifiable to one or other of said correspondents to thereby establish said common key.